IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

TQP DEVELOPMENT, LLC, Plaintiff, v. INTUIT, INC., Defendant.	Case No. 2:12-CV-180-WCB-RSP (LEAD CASE) CONSOLIDATED
TQP DEVELOPMENT, LLC, Plaintiff, v. THE HERTZ CORPORATION Defendant.	Case No. 2:12-CV-702-WCB-RSP

DEFENDANTS INTUIT, INC.'S AND THE HERTZ CORPORATION'S MOTION FOR SUMMARY JUDGMENT OF INVALIDITY UNDER 35 U.S.C. § 101

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s):**

Statutes

Rules

STATEMENT OF ISSUES TO BE DECIDED

Defendants Intuit, Inc. and The Hertz Corporation (collectively, "Movants") move under Fed. R. Civ. P. 56(a) for summary judgment that the asserted claims (1, 3, 6, and 8-10) of U.S. Patent No. 5,412,730 C1 (Dkt. No. 19-1, "the '730 Patent") are invalid under 35 U.S.C. § 101.

STATEMENT OF UNDISPUTED MATERIAL FACTS

A. Conventional prior-art systems in the field of the invention used some transmitter to communicate encrypted data over some communication link to some receiver, where the data was decrypted. (*E.g.*, '730 Patent, 1:12-36; Exhibit A to the accompanying declaration of Philip Warrick ("Warrick Decl.") at 135-39.)

B. Conventional prior-art systems in the field of the invention used some algorithm for generating pseudo-random numbers. (*E.g.*, '730 Patent, 1:27-30; Warrick Decl. Ex. B at 138-39.)

C. Warrick Decl. Exhibit B is an excerpt from a 1982 prior-art text describing a prior-art "synchronous stream cipher" technique in the field of the invention.

D. Warrick Decl. Exhibits A, C, and D are excerpts of testimony of the named inventor, Mr. Jones, while a retained "consultant" of Plaintiff TQP, in other actions brought by TQP asserting the same patent. *See, e.g.*, *TQP Development, LLC v. Merrill Lynch & Co.*, No. 2:08-cv-471-WCB, Dkt. No. 561, at 1-2 (E.D. Tex. July 18, 2012).

E. A human sender and a human receiver of encrypted data can count the blocks of encrypted data sent, to synchronize using a new key value in their shared series of encryption keys.

F. Humans can perform an encryption algorithm on a series of data values using a series of encryption keys, such as the exclusive-or algorithm described in Warrick Decl. Ex. B. (*See also, e.g.*, Warrick Decl. Ex. E.)

I. INTRODUCTION

Section 101 "contains an important implicit exception. Laws of nature, natural phenomena, and abstract ideas are not patentable." *Mayo Collaborative Servs. v. Prometheus*

Labs., Inc., 132 S. Ct. 1289, 1293 (2012) (alteration and internal quotation marks omitted). "[A]bstract intellectual concepts are not patentable, as they are the basic tools of scientific and technological work. And monopolization of those tools through the grant of a patent might tend to impede innovation more than it would tend to promote it." *Id.* (internal citation and quotation marks omitted).

Under this exception, the patent claims asserted here are invalid because they are directed to and seek to preempt a patent-ineligible algorithm and mental process. Humans could perform the claimed algorithm using pen and paper. The claims do not recite computers, the Web, the Internet, databases or memories, routers or other specific network components, or other such computer technology. Indeed, the named inventor, Mr. Jones, has described the patent's alleged improvement as an "abstraction." (Warrick Decl. Ex. A.)

For purposes of this motion, Movants accept Plaintiff's proposed claim constructions in the Joint Claim Construction Statement. (Dkt. Nos. 100, 100-2.)

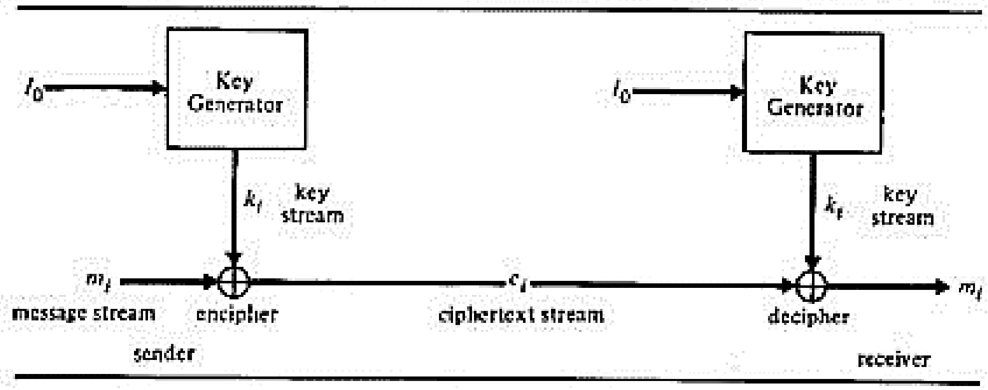
II. <u>THE ASSERTED PATENT</u>

A. <u>Conventional Systems In This Field</u>

The field of the alleged invention is "systems for transmitting enciphered data." ('730 Patent, 1:12-14.) Prior to the filing of the '730 Patent, such systems often employed an algorithm for encrypting (and decrypting) data that used a numeric key known only to the sender and the receiver. The receiver used the same algorithm and same key to decrypt (unscramble) the data that the sender used to encrypt (scramble) the data. The sender and receiver had to share and use the same encryption/decryption algorithm and key(s) or else the attempted decryption would output gibberish. Encrypting the message in this manner protected it from interceptors who lacked the encryption key(s) necessary to decrypt the message, even if they knew the specific type of encryption algorithm being used.

More specifically, such conventional systems computed a series of numbers (representing a scrambled message, or "ciphertext") from two input numbers: one representing the unscrambled data ("clear text" or "plain text") and the other an encryption "key" or series of encryption "keys." The series of new encryption keys often were calculated using an algorithm called a pseudo-random number generator. One type of prior art system, called a "synchronous stream cipher," is depicted in the below diagram from a 1982 text.

FIGURE 3.3 Synchronous stream cipher.



(Warrick Decl. Ex. B at 139.)

In this prior-art system, the sender and receiver use the same encryption algorithm and same series of encryption keys. (*Id.* at 138-39.) They synchronize the value of their initial key by using the same key generator (e.g., a "pseudo-random number generator" algorithm) and the same "seed" value ("I_0"). (*Id.*) The sender and receiver synchronize their advance to the next key in the series by using a new encryption/decryption key for each new character or bit of the message. (*Id.* at 135, 138-39.)

The '730 Patent describes conventional systems as follows:

> Data encryption provides security for transmitted data by scrambling the "clear text" data into "cipher text". Typically, the transmitted data is scrambled in a manner selected by a unique key value (such as a 56-bit binary number) and unscrambled, at the receiving station, by a reverse process that requires the same key value be known.

('730 Patent, 1:15-21.)

As noted, the secrecy of the encryption key allows the content of the message to remain secret. Therefore, it was conventional to change the encryption key frequently so that an eavesdropper who managed to decode the key used to encrypt part of a message would not thereby be able to decipher an entire message or multiple messages. Both parties, of course, had to agree when to advance to the next key in their shared series of keys so that every portion of the encrypted message would be decrypted using the same key used to encrypt it.

The ’730 Patent does not purport to describe an improved encryption algorithm. (Named inventor Michael Jones testified that he did not invent an encryption algorithm. (Warrick Decl. Ex. C at 6:5-12.)) Rather, the patent purports to describe an improved algorithm for the sender and receiver advancing in synchrony to the next key in their shared series of keys.

Several algorithms existed in the prior art for synchronously advancing to the next key. One is the “synchronous stream cipher” depicted and discussed above. The ’730 Patent describes a different prior-art algorithm for synchronously advancing to the next key in the series of keys, *viz.*, sending each new key with an encrypted message:

> For increased data security, the encryption key value may be changed frequently to further reduce the likelihood that an unauthorized party may decipher the data. In such systems, new key values are sent at intervals from the transmitting station to the receiving station. The keys may be generated by a random number generator located at the transmitting end, encrypted in accordance with the currently active key, and transmitted along with the other data. At the receiving station, the encrypted key is extracted from the data stream, deciphered, and substituted at a designated time for the prior key. In such a system, if any of the transmitted keys are deciphered, the successive keys may be deciphered as well, so that all of the transmitted information may be decoded.

(’730 Patent, 1:22-36.)

B. The Claimed Invention

The ’730 Patent claims an algorithm in which sender and receiver in synchronization use new respective encryption/decryption keys when a particular number of blocks of data have been transmitted from sender to receiver. Claim 1, the only independent claim, recites this idea, in part, as follows: “a new one of said key values in said first and said second sequences being produced each time a predetermined number of said blocks are transmitted.” (’730 Patent, 12:46-49 (emphasis added).) The parties’ agreed construction of this claim language is: “a new key value in the first and second sequence is used each time a predetermined number of blocks have been sent from the transmitter over the communication link." (Dkt. No. 100.) In other words, each side counts the number of blocks of data that have been transmitted and uses the next encryption/decryption key when that count reaches a certain predetermined number.

This idea is device agnostic. It does not depend on any particular device. Parties to an encrypted communication can agree to change the encryption key each time an agreed-upon number of bocks are transmitted whether the messages are transmitted by Federal Express, the Internet, or smoke signals. Nor does the patent suggest that its idea improves the performance of any device. Changing the key when a certain number of blocks are transmitted may provide advantages, but it does not make a transmitter (or receiver, or communications link) better at what it does. In other words, there is no functional relationship between this idea and any device. The idea in no way depends on any device, and no device in any way depends on this idea.

The named inventor, Mr. Jones, described the abstract nature of his invention in deposition (emphases added):

> So the block counter as it's shown in the diagram here is an abstraction of an ability to monitor data flowing through a system. So does the invention, if you -- you know, the block counter is not a block counting device. It's an abstraction of a function that a device using this invention could use to monitor the character of the data being transferred so that it can synchronize key changes. (Warrick Decl. Ex. A at 83:6-14.)
>
> A. Well, the transmitter and receiver are also kind of abstractions. (*Id.* at 101:25-102:1.)
>
> A. I believe that the invention that we're looking at today and talking about today uses an abstraction called a block counter. (*Id.* at 182:4-6.)
>
> A. There's a patent here that involves the abstraction of block counting in order to synchronize keys during transmission. The patent office apparently felt that this was a valid patent and I would trust their judgment on that. (*Id.* at 182:21-25.)

Mr. Jones testified that the idea was so simple that one would know it would work by simply identifying the "different abstractions" in a diagram:

> Q. And we talked about it being complete, it's a simple design. Did you ever try your simple design to see if it worked?

> A. The only way that it would have been tested would have been in terms of like a flow diagram so that you take the different pieces of it, you know, the different abstractions that are in there and then, you know, essentially look at it that way. (*Id.* at 30:15-23.)

Mr. Jones has also testified that his claimed invention did not depend on the algorithm used to encrypt or decrypt the messages. (Warrick Decl. Ex. D at 59:6-7, 220:24-221:1.)

C. Claim 1

Plaintiff asserts claims 1, 3, 6, and 8-10 against Movants. Claim 1 is reproduced below (emphases added):

> 1. A method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver comprising, in combination, the steps of:
>
> providing a seed value to both said transmitter and receiver,
>
> generating a first sequence of pseudo-random key values based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link,
>
> encrypting the data sent over said link at said transmitter in accordance with said first sequence,
>
> generating a second sequence of pseudo-random key values based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon said predetermined characteristic of said data transmitted over said link such that said first and second sequences are identical to one another a new one of said key values in said first and said second sequences being produced each time a predetermined number of said blocks are transmitted over said link, and
>
> decrypting the data sent over said link at said receiver in accordance with said second sequence.

Each positively recited step in claim 1 is a calculation or an input to a calculation:

Claim 1 Step	Mathematical Nature
"transmitting data … over a communication link from a transmitter to a receiver" ('730 Patent, 12:26-28.)	Providing data input for a calculation.
"providing a seed value …" (*Id.* at 12:30-31.)	Providing data input for a calculation.
"generating … key values … at" the transmitter (*Id.* at 12:32-37.)	Calculation.

"encrypting the data … at" the transmitter (*Id.* at 12:38-39.)	Calculation.
"generating … key values … at" the receiver (*Id.* at 12:40-49.)	Calculation.
"decrypting the data … at" the receiver (*Id.* at 12:50-51.)	Calculation.

This claim does not restrict who or what performs the recited calculations. The '730 Patent describes some particular devices and circuitry for supposedly performing the needed calculations and transmissions. But none of the claims requires any of those particular devices or circuitry. For example, none of the claims recites the telephone network, the modem, the serial communications controller, or even the microprocessor of Fig. 2 of the '730 Patent. Nor does any claim recite any of the circuitry shown in Figs. 3A-3C of the patent. Nor do the claims recite a general-purpose computer.

In sum, this claim seeks to preempt, in the field of encrypted transmissions, the idea of counting the number of blocks of data transmitted and using that count to synchronize the changing of the encryption key at both sides.

D. The Reexamination Certificate And Claims 3, 6, And 8-10

The Reexamination added dependent claims 3-10. Asserted claims 3, 6, 8, and 9 recite storing or providing additional number values (for possible later use), again without restricting who or what performs these steps. Claim 10 recites performing an additional calculation (to compress data), again without restricting who or what performs this step.

III. THE CLAIMS IN SUIT ARE EVEN FURTHER FROM PATENT ELIGIBILITY THAN THE CLAIMS PREVIOUSLY REJECTED BY THE SUPREME COURT.

A. Governing Supreme Court Precedent

In its most recent § 101 decisions, the U.S. Supreme Court embraced as useful "guideposts" a trilogy of its prior rulings from 1972 to 1981. *See Bilski v. Kappos*, 130 S. Ct. 3218, 3231 (2010); *Prometheus*, 132 S. Ct. at 1294-95. These older decisions—and the claims they rejected or approved—are thus a logical starting point for any analysis under § 101.

1. Benson

In *Gottschalk v. Benson*, 409 U.S. 63 (1972), the Court rejected claims seeking to patent a mathematical algorithm for converting digitally-stored numbers from one encoding format to another. The claims specified that the algorithm used a particular hardware element of a programmable digital computer, called a "reentrant shift register":

> The method of converting signals from binary coded decimal form into binary which comprises the steps of
>
> (1) storing the binary coded decimal signals in a reentrant shift register,
>
> (2) shifting the signals to the right by at least three places, until there is a binary '1' in the second position of said register,
>
> (3) masking out said binary '1' in said second position of said register,
>
> (4) adding a binary '1' to the first position of said register,
>
> (5) shifting the signals to the left by two positions,
>
> (6) adding a '1' to said first position, and
>
> (7) shifting the signals to the right by at least three positions in preparation for a succeeding binary '1' in the second position of said register.

Id. at 73-74 (emphases added).

Despite the requirement of this specific hardware component of a computer, the Court held that the claim improperly sought to protect an abstract idea in violation of § 101. Although the mathematical operations could be performed without a computer, *id.* at 67, the algorithm had "no substantial practical application" other than with programmable digital computers, *id.* at 71. Therefore, tying the algorithm to such devices could not save the claim, because granting the claim "would wholly pre-empt the [algorithm] and in practical effect would be a patent on the algorithm itself." *Id.* at 71-72; *see also Bilski*, 130 S. Ct. at 3230 (explaining *Benson*); *Prometheus*, 132 S. Ct. at 1301 (same).

Similarly, the claims challenged here are directed to mathematical operations for converting numbers from one form to another (and back again). They recite calculations and gathering inputs for those calculations. As in *Benson*, they recite only what is required by the algorithm. Encrypted transmissions necessarily require someone or something to transmit the data ("transmitter") and receive the data ("receiver") over some "communication link." As in *Benson*, reciting these required functions at the highest possible level of generality does not restrict the claims' preemptive footprint, or make them patent eligible. (The parties have agreed that "transmitter" and "receiver" have their "plain meaning," and Plaintiff proposes "plain meaning" for "communication link" as well. (Dkt. No. 114, at 7, 8, 24.))

2. **Flook**

In *Parker v. Flook*, 437 U.S. 584 (1978), the Court rejected this claim:

> 1. A method for updating the value of at least one alarm limit on at least one process variable involved in a process comprising the catalytic chemical conversion of hydrocarbons wherein said alarm limit has a current value of Bo + K wherein Bo is the current alarm base and K is a predetermined alarm offset which comprises:
>
> (1) Determining the present value of said process variable, said present value being defined as PVL;
>
> (2) Determining a new alarm base B_1, using the following equation: B_1=Bo(1.0-F) + PVL(F) where F is a predetermined number greater than zero and less than 1.0;
>
> (3) Determining an updated alarm limit which is defined as B_1 + K; and thereafter
>
> (4) Adjusting said alarm limit to said updated alarm limit value.

Id. at 596-97 (App. Op. Ct.).

Flook's data processing invention used "some type of computer in accordance with a mathematical control equation." *In re Flook*, 559 F.2d 21, 22 (C.C.P.A. 1977), *rev'd sub nom. Parker v. Flook*, 437 U.S. 584. The Supreme Court rejected the claim, despite its assumed use of a computer and its limitation to a specific practical application (catalytic hydrocarbon conversion), because it preempted the algorithm in that field of use and technological environment. *Flook*, 437 U.S. at 594-95; *see also Bilski*, 130 S. Ct. at 3230 (explaining *Flook*); *Prometheus*, 132 S. Ct. at 1298-99 (same). One may not patent an abstract idea even if the claim is limited to a particular field of use or technical environment. *Bilski*, 130 S. Ct. at 3230.

Like the rejected claims in *Flook*, the patent claims challenged here are directed to the use of data processing algorithms including a mathematical algorithm. Both sets of claims' "methods" input data on which some unspecified entity performs a mathematical algorithm to generate output data. Further, neither set of claims restricts the method to any particular device. Any device capable of performing the steps is encompassed by the claims. Therefore, each set of claims preempts the abstract algorithm encompassed by the claim. If anything, the rejected claims in *Flook* had a smaller preemptive footprint than those challenged here. In *Flook*, the claims were limited to a particular application environment, namely a catalytic hydrocarbon conversion process. Not so here, as there is no limit on the content of the transmitted data. It could be financial, engineering, military, medical, or any other type of data.

3. **Diehr**

Movants recognize that algorithms may be patentable in connection with physical limitations. In *Diamond v. Diehr*, 450 U.S. 175 (1981), a patent claim reciting a formula survived § 101 scrutiny because it also positively recited a patentable combination of particular physical steps using a particular physical machine to transform a particular physical article (*viz.*, curing synthetic rubber). *Id.* at 184. These particular and non-algorithmic process steps included "installing rubber in a press," "closing the mold," and "automatically opening the press at the proper time." *Id.* at 187. The claim consequently did not preempt substantially all practical implementations of the recited algorithm in any field of use. *Id.* at 192-93; *see also Prometheus*, 132 S. Ct. at 1298-99 (explaining *Diehr*).

None of the claims challenged here is like the claims approved in *Diehr*. None has a counterpart to the physical, material-transformative steps recited in the *Diehr* claims, such as "installing rubber in a press." The method in *Diehr* transformed physical articles from one state to another. That is not the case here. And, unlike *Diehr*, any steps in the claims challenged here that are not pure calculations or data-gathering were conventional in this field prior to the filing of the patent application.

4. **Bilski**

In *Bilski*, the Supreme Court endorsed the above precedents and unanimously declared ineligible for patenting claims directed to communications ("transactions") among multiple parties. *Bilski,* 130 S. Ct. at 3223-24. The claims were invalid because they "attempt[ed] to patent the use of the abstract idea of hedging risk in the energy market and then instruct the use of well-known random analysis techniques to help establish some of the inputs into the equation." *Id.* at 3231. The Court confirmed that an important, albeit non-exclusive, consideration for policing this abstractness exclusion to patentability is the "machine-or-transformation" test. Specifically, if a patent claim reciting an abstract idea fails to restrict that abstract idea to a particular machine or particular transformation of a particular article, that is "a useful and important clue" that the claim preempts that abstract idea and thus is invalid under 35 U.S.C. § 101. *Bilski*, 130 S. Ct. at 3227.

The claims challenged here require transmission of encrypted data from a transmitter to a receiver over a communication link, but that requirement is a "field of use" restriction that cannot save the claims. Per *Bilski*, gathering data (e.g., providing a seed value) as input to mathematical functions is merely a routine extra-solution step, and inadequate under § 101. Moreover, as explained below, the claims fail the particular-machine-or-transformation "test."

5. **Prometheus**

In *Prometheus*, the Supreme Court unanimously affirmed a trial court's grant of summary judgment invalidating claims of two issued patents under § 101. This ruling supports several points of law on which this motion rests.

First, *Prometheus* rejected the U.S. Government's invitation (echoing some Federal Circuit panel opinions espousing a "coarse filter" view of the abstractness exclusion) to demote § 101 in favor of analyzing validity of patent claims under other sections of the Patent Act. *Prometheus*, 132 S. Ct. at 1304.

Second, *Prometheus* confirmed the continued vitality of the analysis in *Flook*, which dismissed as inadequate any routine or conventional activities recited in a patent claim:

> Moreover, "[t]he chemical processes involved in catalytic conversion of hydrocarbons[,] . . . the practice of monitoring the chemical process variables, the use of alarm limits to trigger alarms, the notion that alarm limit values must be recomputed and readjusted, and the use of computers for 'automatic monitoring-alarming'" were all "well known," to the point where, putting the formula to the side, there was no "inventive concept" in the claimed application of the formula. "[P]ost-solution activity" that is purely "conventional or obvious," the Court wrote, "can[not] transform an unpatentable principle into a patentable process."

Prometheus, 132 S. Ct. at 1299 (quoting *Flook*, 437 U.S. at 589, 594). Applying this principle, the Court dismissed several steps recited in the claims as merely requiring a particular technological environment, or "well-understood, routine, conventional activity previously engaged in by scientists who work in the field." *Id.* at 1298.

Third, *Prometheus* explained that a "narrow and specific" law of nature is no more patent-eligible than a broad one. *Id.* at 1302, 1303. Thus, it is irrelevant whether an algorithm can be expressed briefly or, instead, requires an entire chalkboard.

Finally, *Prometheus* invalidated issued patent claims that enjoyed the same presumption of validity enjoyed by all issued patent claims under 35 U.S.C. § 282. *Prometheus*, 132 S. Ct. at 1305.

IV. THE ANALYTICAL TOOLS ENDORSED BY THE SUPREME COURT <u>DEMONSTRATE THAT THE CHALLENGED CLAIMS VIOLATE § 101.</u>

A. <u>The Claims' Field-Of-Use Restrictions Do Not Save The Claims.</u>

The prohibition against patenting abstract ideas "cannot be circumvented by attempting to limit the use of the formula to a particular technological environment" or adding "insignificant postsolution activity." *Bilski*, 130 S. Ct. at 3230; *accord Prometheus*, 132 S. Ct. at 1294, 1298. Here, as noted, the field of the alleged invention is "systems for transmitting enciphered data." The preamble of claim 1 recites this field as follows: "A method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver." Such a field-of-use restriction cannot save the claims from invalidity under § 101.

B. <u>The Claims Are Directed To And Preempt Mathematical Algorithms.</u>

Patent claims directed to a mathematical algorithm are invalid under § 101. *See*, *e.g.*, *Bilski*, 130 S. Ct. at 3231 ("The concept of hedging, described in claim 1 and reduced to a mathematical formula in claim 4, is an unpatentable abstract idea, just like the algorithms at issue in *Benson* and *Flook*."). An "abstract idea" under § 101 includes both calculations and the selection of particular data for input into a calculation. For example, in *Flook*, part of the abstract idea was to use information representing a current alarm base and a current offset value. *Flook*, 437 U.S. at 596-97 (App.).

Here, the claims are directed to and preempt all practical applications of an abstract algorithm. They are not restricted to a specific application of the abstract idea. As noted, the claimed algorithm concerns changing the encryption key at the sender and receiver in synchrony by counting the blocks transmitted and advancing the key when that count reaches a predetermined number. This idea is useful only in systems that transmit blocks of key-encrypted data from a sender (transmitter) to a receiver, which sender and receiver share the same encryption algorithm and ability to generate the same series of keys—just as the data encoding algorithm in *Benson* was useful only in digital computers. The claims recite merely this required technological environment for this idea. None of the claims restricts who or what performs the steps of the recited "method." As a consequence, the public cannot perform the algorithm recited in the claim without performing the claimed method—not even by performing the calculations by hand using pen and paper.

C. <u>The Claims Encompass A Mental Process.</u>

Patent claims covering a mental process are invalid under § 101. A "mental process" is an abstract idea. "Phenomena of nature, though just discovered, mental processes, and abstract intellectual concepts are not patentable, as they are the basic tools of scientific and technological work." *Benson*, 409 U. S. at 67.

Here, the challenged claims do not prohibit using pen and paper to perform the calculations. The claims recite no computer or computing device of any kind. Nor do they require any calculations requiring a computer. The claims do not specify any particular type of encryption algorithm to encrypt and decrypt the data. Thus, the encryption algorithm could be as simple as the prior-art exclusive-or operation discussed in the 1982 text cited above, which one can easily do with pencil and paper, as demonstrated by Plaintiff in its own infringement contentions. (*See* Warrick Decl. Ex. B at 50; Warrick Decl. Ex. E.) Nor do the claims require any particular algorithm for calculating pseudo-random numbers from a seed value. The mathematician John von Neumann described such an algorithm, called the middle-square method, in a 1951 paper: (1) take any number as the seed value, (2) square it, (3) remove the middle digits of the resulting number as the pseudo-random number, (4) then use that number as the seed for the next iteration. (*See* Warrick Decl. Ex. F.) A human can not only do this with pen and paper, but also perform this calculation entirely in the mind.

D. **The Claims Do Not Require A Particular Machine.**

The particular-machine-or-transformation test asks whether a claimed method "(1) [is] tied to a particular machine or apparatus, or (2) it transforms a particular article into a different state or thing." *Bilski*, 130 S. Ct. at 3225. "This Court's precedents establish that the machine-or-transformation test is a useful and important clue, an investigative tool, for determining whether some claimed inventions are processes under § 101. The machine-or-transformation test is not the sole test for deciding whether an invention is a patent-eligible 'process.'" *Id.* at 3227.

Here, none of the claims ties the claimed method to a particular machine. The claims do not specify or restrict who or what performs any of the recited calculations. Nor do they restrict who or what sends, communicates, or receives the data. Plaintiff may argue that the claims' "transmitter," "receiver," and "communication link" constitute a "particular machine." They do not for several reasons.

First, they do not mandate any particular machine to perform the functions of transmitting, communicating, and receiving the data. For example, the "transmitter" could be a person, an optical telegraph (invented in 1794), an electric telegraph, an electro-magnetic telegraph (e.g., using Morse code), a teleprinter, a facsimile machine, a land-line telephone, a cell phone, a TV broadcast system, or a computer modem. Indeed, the "transmitter," "receiver," and "communications link" could be mechanisms for performing those functions which had not even been invented when the patent issued. In other words, the claim does not mandate a particular type of machine or apparatus for performing the functions of transmitting, communicating, or receiving the data. Instead, the claims use the most generic, functional language possible ("transmitter," "communication link," and "receiver") for something (anything) capable of performing the steps of transmitting, communicating and receiving data.

Second, even if the claim terms "transmitter," "receiver," or "communication link" were considered to be a particular machine, the abstract idea of using the next key when the transmitted blocks of encrypted data reaches a predetermined number necessarily requires something or someone to transmit the data, something or someone to communicate it, and something or someone to receive it. Therefore, as in *Benson*, these claim terms do not in fact limit the claim; they do not reduce the "pre-emptive footprint" of the claim. *See In re Bilski*, 545 F.3d 943, 953-54 (Fed. Cir. 2008) (en banc) (discussing *Benson*, 409 U.S. at 65, 70-72), *aff'd sub nom. Bilski v. Kappos*, 130 S. Ct. 3218.

Third, even if these claim terms—"transmitter," "receiver," or "communication link"—were deemed a particular machine, they at most limit use of the recited mathematical operations to a field of use, namely "systems for transmitting enciphered data" as stated in the patent ('730 Patent, 1:12-14.) Such a field-of-use restriction cannot satisfy § 101.

E. **The Claims Do Not Require Transforming a Particular Article.**

These claims also fail the "particular transformation" prong of this "important clue" to patent eligibility. None of the challenged patent claims requires a particular article. As in *Benson*, they transform numbers from one form to another. They do not even require the numbers to be represented in any physical form such as an electrical, magnetic, or optical signal or marking on a page of paper. Nor do they require any particular transformation of a particular article into a different state. For example, they do not require numbers stored in one's mind to be written down on paper, or entered into a computer, or otherwise transformed into a different storage or transmission medium. Nor do these claims require that the data represent any physical, tangible objects, or require a particular visual depiction of a physical object on a display. *Cf. In re Abele*, 684 F.2d 902, 908-09 (C.C.P.A. 1982), *abrogated on other grounds by In re Bilski*, 545 F.3d at 959.

V. THE DEPENDENT CLAIMS ADD NOTHING TO CHANGE THE ANALYSIS.

The challenged dependent claims—added in reexamination—at most narrow the algorithm recited in claim 1, without restricting implementation of that algorithm to any particular, unconventional machine. Claims 3, 6, 8, and 9 recite storing or providing additional number values (for possible later use), again without restricting who or what performs these steps. Claim 10 recites performing an additional calculation, again without restricting who or what performs this step.

These claims may narrow the algorithm (abstract idea), but that is irrelevant to the § 101 analysis. A patent is no more permitted to preempt a narrow idea than it is permitted to preempt a broad idea. The abstract idea, mental process, or mathematical formula might be quite specific and narrow, as in the *Benson*, *Flook* and *Bilski* claims. "[T]he particular laws of nature that its patent claims embody are narrow and specific," "but the patent claims that embody them nonetheless implicate this concern" that patent laws not inhibit future innovation. *Prometheus*, 132 S. Ct. at 1302, 1303.

VI. THIS ISSUE IS RIPE FOR DECISION NOW

"Whether a claim is drawn to patent-eligible subject matter under § 101 is an issue of law . . . ." *In re Bilski*, 545 F.3d at 950-51. There are no genuinely disputed material facts. There is no need for further discovery. As noted, for purposes of this motion, Movants accept Plaintiff's proposed constructions. None of them saves the claims from invalidity under § 101.

Respectfully submitted,

Dated: December 26, 2013

By: */s/ John D. Vandenberg*
Elisabeth V. Bechtold (OR Bar No. 116303)
eliza.bechtold@klarquist.com
Scott E. Davis (OR Bar No. 022883)
scott.davis@klarquist.com
Derrick W. Toddy (OR Bar No. 072043)
derrick.toddy@klarquist.com
John D. Vandenberg (OR Bar No. 893755)
john.vandenberg@klarquist.com

Philip Warrick (OR Bar No. 116191)
philip.warrick@klarquist.com
KLARQUIST SPARKMAN, LLP
121 S.W. Salmon Street, Suite 1600
Portland, Oregon 97204
Telephone: (503) 595-5300
Facsimile: (503) 595-5301

COUNSEL FOR DEFENDANT
INTUIT, INC.

By: *\/s/ Wasif Qureshi*
Neil J. McNabnay
Texas Bar No. 24002583
mcnabnay@fr.com
David B. Conrad
conrad@fr.com
Texas Bar No. 24049042
Ricardo J. Bonilla
Texas Bar No. 24082704
rbonilla@fr.com
James Y. Wang
Texas Bar No. 24084042
wang@fr.com
1717 Main Street, Suite 5000
Dallas, Texas 75201
Telephone: 214.747.5070
Facsimile: 214.747.2091

Wasif Qureshi
qureshi@fr.com
Texas Bar No. 24048155
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 654-5300 – Telephone
(713) 652-0109 - Facsimile

COUNSEL FOR DEFENDANT
THE HERTZ CORPORATION

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on December 26, 2013 a true and correct copy of the above and foregoing document has been served on all counsel of record who are deemed to have consented to electronic service via the Court's CM/ECF system per Local Rule CV-5(a)(3).

/s/ John D. Vandenberg
John D. Vandenberg